|  |  |
| --- | --- |
|  | Dopo la compilazione almeno: A USO INTERNO |

|  |
| --- |
|  |

Regolamento dei privati per il trattamento dei dati

< Nome del progetto / dell’oggetto da proteggere >

|  |
| --- |
|  |

|  |  |
| --- | --- |
| Classificazione | **A USO INTERNO** / CONFIDENZIALE / SEGRETO |
| Stato | **In corso di elaborazione** / in corso di verifica / approvato |
| Numero del progetto |  |
| Capoprogetto (CP BP) |  |
| Versione | Dal modello V2.1 - P042-Hi04 - Regolamento per il trattamento dei dati |
| Data |  |
| Committente |  |
| Elaborato da |  |

Controllo delle modifiche

|  |  |  |  |
| --- | --- | --- | --- |
| Versione | Data | Descrizione / Osservazioni | Nome |
| 0.1 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Distribuzione

|  |  |  |
| --- | --- | --- |
| Funzione | Nome | Organizzazione / Impresa |
| Consulenti per la protezione dei dati |  |  |
| CISO |  |  |
|  |  |  |
|  |  |  |

Indice

1 Considerazioni generali 4

1.1 Descrizione 4

1.2 Scopo del regolamento dei privati per il trattamento dei dati 4

1.3 Adeguamento 4

1.4 Ausili 5

1.5 Autorizzazione 6

2 Regolamento dei privati sul trattamento 7

2.1 Informazioni generali 7

2.1.1 Scopo del trattamento dei dati 7

2.1.2 Categorie di persone interessate e categorie di dati personali trattati 7

2.2 Organizzazione interna 7

2.2.1 Titolare del trattamento 7

2.2.2 Responsabile del trattamento 8

2.2.3 Utenti e accesso ai dati 8

2.2.3.1 Cerchia di utenti 8

2.2.3.2 Diritti di accesso 8

2.2.3.3 Ruoli 8

2.2.3.4 Processo relativo ai diritti di accesso 8

2.3 Procedura di trattamento e di controllo dei dati 9

2.3.1 Trattamento dei dati personali 9

2.3.1.1 Processi aziendali 9

2.3.1.2 Comunicazione dei dati e interfacce 9

2.3.1.3 Controllo dei dati personali registrati 10

2.3.1.4 Processi / Procedure per il trattamento dei dati 10

2.3.2 Durata di conservazione, archiviazione e cancellazione 10

2.3.2.1 Durata di conservazione 10

2.3.2.2 Archiviazione 10

2.3.2.3 Cancellazione 10

2.3.3 Diritti delle persone interessate 11

2.4 Misure atte a garantire la sicurezza dei dati 11

3 Allegato 12

3.1 Registro delle attività di trattamento 12

3.2 Valutazione d’impatto sulla protezione dei dati 13

3.3 Piano dei diritti di accesso / Matrice delle autorizzazioni 13

3.4 Elenco dei documenti 15

3.5 Abbreviazioni 16

3.6 Termini 17

# Considerazioni generali

## Descrizione

Descrizione del trattamento automatizzato del progetto TIC.

## Scopo del regolamento dei privati per il trattamento dei dati

Il **titolare privato del trattamento e il suo responsabile privato** (cfr. art. 5 OPDa) stabiliscono un regolamento per i trattamenti automatizzati se:

* trattano su grande scala dati personali degni di particolare protezione; oppure
* eseguono una profilazione a rischio elevato.

Il regolamento contiene in particolare indicazioni

* sull’organizzazione interna,
* sulla procedura di trattamento e di controllo dei dati, nonché
* sui provvedimenti per garantire la sicurezza dei dati.

Contiene anche l’elenco di tutta la documentazione relativa alla pianificazione, alla realizzazione e alla gestione della raccolta di dati. Al regolamento si devono allegare il registro delle attività di trattamento (secondo art. 12 e art. 15 LPD) e una valutazione d’impatto sulla protezione dei dati appositamente effettuata (secondo art. 22 LPD).

Scopo del regolamento è rendere possibile un’analisi e una valutazione a regola d’arte degli eventuali rischi legati alla protezione dei dati.

Il titolare privato del trattamento e il suo responsabile privato sono tenuti ad aggiornare periodicamente il regolamento. In caso di nomina di un consulente per la protezione dei dati, questi deve poter disporre di tale regolamento.

## Adeguamento

Il regolamento per il trattamento dei dati deve essere il più possibile conciso e comprensibile, in modo che la descrizione della raccolta automatizzata di dati possa essere compresa e valutata anche da persone non esperte in materia (principio).

Il regolamento deve essere tanto più esaustivo quanto più aumenta il volume o la sensibilità dei dati personali da trattare. A meno che non siano già contenuti in un piano SIPD, gli aspetti più importanti dal punto di vista della protezione dei dati e della sicurezza delle informazioni devono essere descritti nel regolamento per il trattamento. Per informazioni più dettagliate si rimanda ai documenti di approfondimento.

È importante non copiare il contenuto dei documenti esistenti, ma fare riferimento ad essi con informazioni precise e allegare tali documenti. Il Regolamento non deve essere un esercizio di copia e riproduzione.

Il testo in blu funge da ausilio alla compilazione del documento.

## Ausili

I seguenti documenti fungono da supporto per l’elaborazione del regolamento per il trattamento dei dati:

**Ausili:**

* [Direttive del delegato federale alla cibersicurezza sulla procedura di sicurezza e sui relativi mezzi ausiliari a livello di Confederazione](https://www.ncsc.admin.ch/ncsc/it/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html), NCSC
* Misure tecniche e organizzative (TOM) (nel centro di informazione sulla protezione dei dati dell'IFPDT)

## Autorizzazione

Le firme di autorizzazione devono essere apposte prima dell’inizio dell’attività.

Con la propria firma, il consulente per la protezione dei dati conferma di aver controllato il regolamento per il trattamento. Il consulente ha verificato in particolare che il documento sia stato compilato in ogni sua parte e che tutte le misure richieste siano documentate; ha inoltre analizzato le indicazioni in modo critico per stabilirne la coerenza e l’esattezza nel contesto del trattamento dei dati.

Con la propria firma, il titolare del trattamento approva il relativo regolamento.

|  |  |
| --- | --- |
| Data / Nome / Firma  **Consulente per la protezione dei dati**: | …………………………………………………...…... |
| Data / Nome / Firma  **Titolare del trattamento**: | …………………………………………………...…... |
|  |  |

**È possibile apporre altre firme.**

**Le firme possono essere apposte anche in forma elettronica (in un file PDF).**

# Regolamento dei privati sul trattamento

## Informazioni generali

### Scopo del trattamento dei dati

(art. 6 cpv. 3 LPD in combinato disposto con art. 1 cpv. 2 lett. b OPDa, art. 6 cpv. 4–5, art. 7 cpv. 3, art. 12 cpv. 2 LPD)

Si devono descrivere scopo, tipo, entità e circostanze del trattamento, oltre al numero e tipo di persone coinvolte.

Nella premessa si devono illustrare brevemente i motivi per cui si intende allestire un sistema e descrivere lo scopo (o gli scopi) nonché lo stato auspicato.

### Categorie di persone interessate e categorie di dati personali trattati

(art. 6 cpv. 6 e 7, art. 12 cpv. 2, art. 19 LPD; art. 1 cpv. 2 lett. a, art. 13 OPDa)

In merito al contenuto dei dati trattati occorre rispondere alle seguenti domande:

* Quale tipologia di dati personali viene trattata (dati personali, dati personali degni di particolare protezione, profilazione a rischio elevato, altri)?
* Quali categorie (o «gruppi») di persone e dati personali sono trattate?
* Come vengono raccolti i dati personali?

## Organizzazione interna

(art. 9, 10, 12–15 LPD; art. 7, 8, 17, 23 OPDa)

### Titolare del trattamento

Indicare l’identità del titolare del trattamento (compresa la rappresentanza in Svizzera in caso di titolari privati con sede o domicilio all’estero) e, se presente, l’identità del consulente per la protezione dei dati per il trattamento dei dati, compresa la rispettiva organizzazione interna. Occorre indicare anche a chi competono le procedure di trattamento dei dati e di controllo nonché chi è responsabile della definizione (ad es. tramite valutazione d’impatto sulla protezione dei dati) e dell’attuazione dei provvedimenti finalizzati a garantire la sicurezza dei dati.

Indicazioni su:

Titolare del trattamento:

Rappresentanza in Svizzera in caso di titolari privati con sede o domicilio all’estero:

Consulente per la protezione dei dati:

### Responsabile del trattamento

Si devono indicare il responsabile del trattamento competente e le persone di riferimento responsabili.

Indicazioni su:

Responsabile del trattamento:

Persona di riferimento FP/Responsabile del trattamento:

### Utenti e accesso ai dati

#### Cerchia di utenti

Riportare le categorie (o «gruppi») di tutte le unità organizzative o posizioni autorizzate all’accesso.

Eventualmente, inserire qui un rimando alla matrice della comunicazione del piano SIPD.

#### Diritti di accesso

Elencare e descrivere brevemente il tipo e l’estensione dell’accesso degli utenti alla raccolta di dati nonché i campi dei dati. Se esiste già una matrice delle autorizzazioni (o un piano dei diritti di accesso), deve essere aggiunta al regolamento per il trattamento come allegato.

#### Ruoli

A quali ruoli sono stati assegnati diritti di accesso (ad es. collaboratore specializzato, amministratore) e quali diritti di accesso sono stati attribuiti a ogni ruolo (interrogazione, elaborazione, stampa, nessun accesso, altro)?

#### Processo relativo ai diritti di accesso

Qui occorre descrivere le modalità (processo e responsabilità) relative all’assegnazione e alla revoca dei diritti di accesso, fornendo le informazioni seguenti:

* Chi è responsabile dell’assegnazione e della revoca dei diritti di accesso?
* Chi controlla regolarmente i diritti di accesso assegnati e li aggiorna?
* Estensione dei diritti di accesso?
* Esiste un processo per l’assegnazione e la revoca dei diritti di accesso?
* Iter del processo?
* Il processo è gestito a livello centralizzato?

## Procedura di trattamento e di controllo dei dati

(art. 6–14, 16, 19, 21, 22, 24, 25, 28, 30, 32 LPD; art. 1–5, 9–13, 15–18, 20, 22–24 OPDa)

Argomenti:

Distruzione dei dati nel momento in cui non sono più necessari allo scopo del trattamento

Misure atte alla rettifica dei dati personali

Consenso al trattamento dei dati personali

Protezione dei dati attraverso la tecnologia e preimpostazioni orientate alla protezione dei dati

Misure di sicurezza dei dati

Rapporto con il responsabile del trattamento

Coinvolgimento del consulente per la protezione dei dati

Gestione del registro delle attività di trattamento

Utilizzo di certificazioni

Condizioni per la comunicazione legale dei dati personali all’estero

Obbligo di informare sulla raccolta di dati personali

Obbligo di informare sulle decisioni individuali automatizzate

Valutazione d’impatto sulla protezione dei dati

Segnalazione di violazioni della sicurezza dei dati

Configurazione del diritto d’accesso

Diritto alla consegna o alla trasmissione dei dati

Controllo e responsabilità in caso di trattamento congiunto dei dati personali

Comunicazione dei dati personali

### Trattamento dei dati personali

#### Processi aziendali

In questa sezione si devono documentare e/o rappresentare graficamente i processi aziendali di raccolta di dati più importanti dal punto di vista della protezione dei dati.

#### Comunicazione dei dati e interfacce

Le interfacce con altri oggetti da proteggere come sistemi, applicazioni, software ecc. devono essere rappresentate graficamente qui. È possibile inserire anche un rimando a un eventuale piano SIPD che contenga già una panoramica di questo tipo.

La descrizione delle interfacce deve contenere le seguenti informazioni relative alla trasmissione (comunicazione) di dati:

* Da chi provengono i dati personali?
* Chi riceve i dati personali?
* A che scopo vengono trasmessi i dati personali?
* Quali categorie (o «gruppi») di dati personali vengono trasmesse?
* Con quale frequenza vengono trasmessi i dati personali?
* Chi avvia la procedura di trasmissione?
* Con l’aiuto di quale strumento vengono trasmessi i dati personali?

Gli scopi per cui i dati personali vengono regolarmente comunicati si devono evincere dalla descrizione delle interfacce.

#### Controllo dei dati personali registrati

Chi controlla l’esattezza dei dati personali? Esiste un processo in tal senso? Questi dati vengono controllati e rettificati regolarmente?

#### Processi / Procedure per il trattamento dei dati

Si devono definire e descrivere i processi di rettifica, blocco, anonimizzazione, registrazione, conservazione, archiviazione e distruzione dei dati.

### Durata di conservazione, archiviazione e cancellazione

#### Durata di conservazione

Si devono chiarire le seguenti questioni:

* Per quanto tempo si possono o devono conservare i dati personali registrati o le categorie («gruppi») di dati personali?
* Luogo e responsabilità della conservazione dei dati personali?
* In quale momento vengono cancellati o devono essere consegnati all’Archivio federale?

#### Archiviazione

Si devono definire qui le modalità tecniche e organizzative (formato dei file, interfacce) per offrire all’Archivio federale di riprendere i dati personali o per la loro trasmissione all’Archivio stesso.

#### Cancellazione

In quale momento i dati personali non più necessari vengono cancellati dalla raccolta di dati? Questa formulazione deve essere stabilita d’intesa con il responsabile della sicurezza delle informazioni e il responsabile delle applicazioni.

### Diritti delle persone interessate

Si deve stabilire in particolare a chi debba rivolgersi la persona interessata (persona di riferimento/destinatario) e la relativa procedura interna (processo).

Si devono creare gli strumenti e le procedure per l’esercizio del diritto alla rettifica, alla distruzione e al blocco nonché del diritto di aggiungere una menzione del carattere contestato. Devono sussistere ed essere attuabili appositi strumenti per il blocco della comunicazione a terzi.

L’obbligo di informare sulla raccolta di dati personali a opera di privati deve essere considerato e regolato (art. 19 e 20 LPD).

## Misure atte a garantire la sicurezza dei dati

(art. 7, 8, 10–13, 22, 24 LPD; art. 1–5, 15, 23 OPDa)

Qui si devono elencare le misure tecniche e organizzative che garantiscono una protezione dei dati adeguata e che non sono già contenute nel piano SIPD.

# Allegato

## Registro delle attività di trattamento

Il titolare del trattamento, il rappresentante in Svizzera del titolare privato con sede all’estero e il responsabile del trattamento tengono ciascuno un registro delle loro attività di trattamento.

Il registro del titolare del trattamento e quello del rappresentante contengono almeno:

* l’identità del titolare del trattamento;
* lo scopo del trattamento;
* una descrizione delle categorie di persone interessate e delle categorie di dati personali trattati;
* le categorie di destinatari;
* se possibile, la durata di conservazione dei dati personali o i criteri per determinare tale durata;
* se possibile, una descrizione generale dei provvedimenti tesi a garantire la sicurezza dei dati personali secondo l’articolo 8 LPD;
* nel caso in cui i dati siano comunicati all’estero, le informazioni sullo Stato destinatario e le garanzie secondo l’articolo 16 capoverso 2 LPD.

Il registro del responsabile del trattamento contiene informazioni sull’identità del responsabile e del titolare, sulle categorie dei trattamenti che vengono svolti su incarico del titolare, nonché almeno:

* se possibile, una descrizione generale dei provvedimenti tesi a garantire la sicurezza dei dati personali secondo l’articolo 8 LPD;
* nel caso in cui i dati siano comunicati all’estero, le informazioni sullo Stato destinatario e le garanzie secondo l’articolo 16 capoverso 2 LPD.

Il Consiglio federale prevede eccezioni ai registri delle attività di trattamento per le imprese che impiegano meno di 250 collaboratori e per i quali il trattamento dei dati comporta un rischio esiguo di violazione della personalità delle persone interessate.

## Valutazione d’impatto sulla protezione dei dati

In determinate condizioni, il titolare del trattamento deve redigere una valutazione d’impatto sulla protezione dei dati.

In tal caso, se ne deve allegare una copia al regolamento sul trattamento.

## Piano dei diritti di accesso / Matrice delle autorizzazioni

Il piano dei diritti di accesso o la matrice delle autorizzazioni devono essere inseriti nel regolamento per il trattamento come allegati.

Segue un esempio semplificato di una matrice delle autorizzazioni.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Nome campo dati | Azienda | | | | | | Filiale | | | | | | Terzi | |
|  | UA I | UA II | UA III | … | … | … | Finanza | … | … | … | … | … | … | … |
|  | | | | | | | | | | | | | | |
| I. Dati di base | | | | | | | | | | | | | | |
| Cognome/i | I | I | T | … | … | … | I | … | … | … | … | … | … | … |
| Nome/i | I | I | T | … | … | … | I | … | … | … | … | … | … | … |
| Data di nascita |  | I | I | … | … | … | I | … | … | … | … | … | … | … |
| Nazionalità |  | I | I | … | … | … | T | … | … | … | … | … | … | … |
| … | … | … | … | … | … | … | … | … | … | … | … | … | … | … |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| II. Informazioni sul dossier | | | | | | | | | | | | | | |
| Titolare del dossier | T | T | T | … | … | … | I | … | … | … | … | … | … | … |
| Stato del dossier | T | T | T | … | … | … |  | … | … | … | … | … | … | … |
| Numero di riferimento | I | T | T | … | … | … | T | … | … | … | … | … | … | … |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| III. Titolo X | | | | | | | | | | | | | | |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Livelli di accesso**

I = Interrogazione

T = Trattamento

vuoto = nessun accesso

altro

**Unità amministrative**

UA I: ad es. servizio legale dell’UA interessata

UA II: ad es. collaboratore specializzato dell’UA interessata

UA III: ad es. amministratore dell’UA interessata

…

Filiale: ad es. Finanza

…

## Elenco dei documenti

Comprende l’elenco di tutte le leggi, ordinanze, istruzioni, regolamentazioni, specifiche tecniche ecc. rilevanti per la raccolta di dati in oggetto, inclusi i documenti aziendali (pubblici o interni).

|  |  |
| --- | --- |
| Tipo di documento | Titolo |
| Leggi | [Legge federale del 25 settembre 2020 sulla protezione dei dati (LPD; RS *235.1*)](http://www.admin.ch/ch/i/sr/c235_1.html) |
| Ordinanze | [Ordinanza del 31 agosto 2022 sulla protezione dei dati (OPDa; RS *235.11*)](https://www.fedlex.admin.ch/eli/cc/2022/568/it) |
| Istruzioni |  |
| Documenti  propri | Piano dei diritti di accesso |
|  | Rappresentazione del flusso di dati / Diagramma del flusso di dati |
|  | Struttura architettura IT |
|  | … |

## Abbreviazioni

|  |  |
| --- | --- |
| Abbreviazione | Significato |
| art. | articolo |
| BP | beneficiario di prestazioni |
| CISO | Chief Information Security Officer |
| cpv. | capoverso |
| FP | fornitore di prestazioni |
| IFPDT | Incaricato federale della protezione dei dati e della trasparenza |
| lett. | lettera |
| LPD | Legge federale sulla protezione dei dati (RS *235.1*) |
| NCSC | Centro nazionale per la cibersicurezza |
| OPDa | Ordinanza sulla protezione dei dati (RS *235.11*) |
| Piano SIPD | Piano per la sicurezza delle informazioni e la protezione dei dati |
| RS | Raccolta sistematica del diritto federale |
| TIC | Tecnologie dell’informazione e della comunicazione |
| UA | Unità amministrativa |
| … | … |

## Termini

|  |  |
| --- | --- |
| Termine | Significato |
| Trattamento | Qualsiasi operazione relativa a dati personali, indipendentemente dai mezzi e dalle procedure impiegati, segnatamente la raccolta, la registrazione, la conservazione, l’utilizzazione, la modificazione, la comunicazione, l’archiviazione, la cancellazione o la distruzione di dati (cfr. art. 5 lett. d LPD). |
| Comunicazione | La trasmissione di dati personali o il fatto di renderli accessibili (cfr. art. 5 lett. e LPD). |
| Dati personali degni di particolare protezione | Dati concernenti le opinioni o attività religiose, filosofiche, politiche o sindacali; dati concernenti la salute, la sfera intima o l’appartenenza a una razza o a un’etnia; dati genetici; dati concernenti le misure d’assistenza sociale; dati concernenti perseguimenti e sanzioni amministrativi e penali; dati biometrici che identificano in modo univoco una persona fisica (art. 5 lett. c LPD). |
| Violazione della sicurezza dei dati | Violazione della sicurezza in seguito alla quale, in modo accidentale o illecito, dati personali vengono persi, cancellati, distrutti, modificati oppure divulgati o resi accessibili a persone non autorizzate (art. 5 lett. h LPD). |
| Titolare del trattamento | Il privato o l’organo federale che, singolarmente o insieme ad altri, determina lo scopo e i mezzi del trattamento (art. 5 lett. j LPD). |
| Responsabile del trattamento | Il privato o l’organo federale che tratta dati personali per conto del titolare del trattamento (art. 5 lett. k LPD). |
| Dati personali, persona interessata | Tutte le informazioni concernenti una persona fisica identificata o identificabile (art. 5 lett. a e b LPD). |
| Profilazione | Trattamento automatizzato di dati personali consistente nell’utilizzazione degli stessi per valutare determinati aspetti personali di una persona fisica, in particolare per analizzare o prevedere aspetti concernenti il rendimento professionale, la situazione economica, la salute, le preferenze, gli interessi, l’affidabilità, il comportamento, i luoghi di permanenza e gli spostamenti di tale persona (art. 5 lett. f LPD). |
| Profilazione a rischio elevato | Profilazione che comporta un rischio elevato per la personalità o i diritti fondamentali della persona interessata poiché comporta un collegamento tra dati che permette di valutare aspetti essenziali della personalità di una persona fisica (art. 5 lett. g LPD). |
| … | … |